

DODATEK č. 3
č.j.: PPR-8824-61/ČJ-2018-990656

k Rámcové dohodě o poskytování technické podpory, podpory provozu a rozvoje
Informačního systému cizinců, č. j. PPR-8824-45/ČJ-2018-990656

Smluvní strany:

Česká republika – Ministerstvo vnitra


Sídlo: Nad Štolou 936/3, PSČ 170 34, Praha
IČO: 00007064
DIČ: CZ00007064
Zastoupená: plk. Mgr. Branislavem Samkem, ředitelem Národního centra
informačních a komunikačních technologií Policejního prezidia
České republiky

Korespondenční adresa: Policejní prezidium ČR, Národního centra informačních
a komunikačních technologií, poštovní schránka 62/NCIKT,
Strojnická 27, 170 89 Praha 7

(dále jen „Objednatel“)

a

ICZ a.s.

Sídlo: Na hřebenech II 1718/10, Nusle, 140 00 Praha 4
IČO: 25145444
DIČ: CZ699000372
Zastoupená: 

Korespondenční adresa: Na hřebenech II 1718/10, Nusle, 140 00 Praha 4

Obchodní společnost zapsaná v obchodním rejstříku vedeném Městským soudem v Praze
pod sp. zn. B4840.

(dále jen „Dodavatel“)

(společně dále také jen „Smluvní strany“)

uzavírají níže uvedeného dne, měsíce a roku tento dodatek č. 3 k Rámcové dohodě ze dne
20. 09. 2018, č. j. PPR-8824-45/ČJ-2018-990656 (dále jen „Dodatek“):

1. ÚVODNÍ USTANOVENÍ

1.1. Tento Dodatek se uzavírá k Rámcové dohodě ze dne 20. 9.2018, č. j. PPR-8824-45/ČJ-2018-
990656, jejímž předmětem je poskytování technické podpory, podpory provozu a rozvoje
Informačního systému cizinců (dále jen „Dohoda“).

- 1.2. Tento Dodatek se uzavírá v souladu s § 222 zák. č. 134/2016 Sb., o zadávání veřejných zakázek, kdy změny uvedené v čl. 2 tohoto Dodatku nenaplní znaky podstatné změny závazku dle § 222 odst. 3 ZZVZ.

2. PŘEDMĚT DODATKU

- 2.1. Tímto Dodatkem se nahrazuje čl. 11 odst. 11. 2. Dohody, a to následujícím zněním:

„Kromě zákonných zástupců Smluvních stran, další kontaktní osoby oprávněné jednat ve věcech plnění poskytovaného dle této Dohody včetně práva podepsat akceptační protokol:

za Dodavatele:



za Objednatele:



- 2.2. Smluvní strany se dohodly, že čl. 3. odst. 3. 3. Dohody se nahrazuje následujícím zněním:

„Celková cena plnění dle Prováděcích smluv uzavřených dle této Dohody (tj. součet smluvních cen uzavřených prováděcích smluv) nesmí přesáhnout 232.419.400,- Kč bez DPH (dvě stě třicet dva miliony čtyři sta devatenáct tisíc čtyři sta korun českých). Počty jednotek uvedené u jednotlivých plnění v Příloze č. 3 Dohody jsou předpokládány a počet jednotek je čerpán dle aktuální potřeby Objednatele s tím, že se nepřekročí celková cena za Plnění A a celková cena za Plnění B.“

- 2.3. Smluvní strany se dále dohodly, že se součástí Dohody nově stává Příloha č. 5, která upravuje bezpečnostní opatření pro smluvní vztahy a její znění je uvedeno v příloze tohoto Dodatku.

3. ZÁVĚREČNÁ USTANOVENÍ

- 3.1. Ostatní ustanovení Dohody se nemění.
- 3.2. Tento Dodatek nabývá platnosti dnem podpisu Smluvními stranami a účinnosti dnem jeho uveřejnění v registru smluv.
- 3.3. Tento Dodatek je podepsán oběma Smluvními stranami elektronickým podpisem.
- 3.4. Nedílnou součástí tohoto Dodatku je Příloha č.5 – „Bezpečnostní opatření pro smluvní vztahy“.


V Praze dne (dle el. podpisu)

V Praze dne (dle el. podpisu)

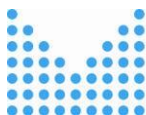
Objednatel:

Dodavatel:

.....
 Ministerstvo vnitra – Česká republika
 Zástupce: plk. Mgr. Branislav Samek
 Funkce: ředitel NCIKT PP ČR

ICZ a.s.
 Zástupce: 
 Funkce: předseda představenstva





BEZPEČNOSTNÍ OPATŘENÍ PRO SMLUVNÍ VZTAHY

1. Úvod

Tato příloha č. 5 (dále také jen „Příloha“) k Rámcové dohodě č. j. PPR-8824-45/ČJ-2018-990656 (dále také jen „Dohoda“) popisuje bezpečnostní požadavky na poskytování technické podpory, podpory provozu a rozvoje Informačního systému cizinců (CIS), zejména pro naplnění požadavků vyplývajících se zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „ZKB“), a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti (dále jen „VKB“)) pro systém kritické informační infrastruktury resortu MV.

2. Bezpečnostní požadavky

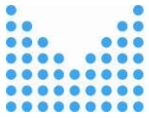
2.1. Účel

1. Tato Příloha stanoví způsoby a úroveň realizace bezpečnostních opatření pro Dodavatele a určuje vzájemný vztah odpovědnosti za zavedení a kontrolu bezpečnostních opatření mezi Objednatelem a Dodavatelem.
2. Smluvní strany se dohodly, že pokud to bude potřebné ke splnění požadavků ZKB, VKB, či souvisejících právních předpisů z oblasti bezpečnosti informací, uzavřou bez zbytečného odkladu po výzvě kterékoli Smluvní strany písemný dodatek k Dohodě zohledňující takové požadavky.

2.2. Obecné bezpečnostně provozní požadavky

Dodavatel se při poskytování plnění pro Objednatele zavazuje plnit následující povinnosti:

1. Postupovat v souladu s účinnými právními předpisy, zejména pak požadavky vyplývajícími pro Dodavatele, jakožto významného dodavatele systému kritické informační infrastruktury, ze ZKB a VKB a reflektovat případné novely dotčených právních předpisů či novou právní úpravu, a bezpečnostními politikami stanovenými systémem řízení bezpečnosti informací (ISMS) Objednatele dle specifikace předmětu veřejné zakázky.
2. Jmenovat nejpozději do tří pracovních dnů po dni účinnosti této Přílohy zodpovědnou kontaktní osobu pro potřeby zajištění plnění bezpečnostních požadavků vyplývajících z této Přílohy, Dohody, Prováděcí smlouvy a související komunikace mezi Smluvními stranami (dále také jen „Kontaktní osoba pro bezpečnost na straně Dodavatele“). Kontaktní osobu pro bezpečnost na straně Dodavatele sdělí písemně Objednateli v téže lhůtě.
3. Zajistit, aby Kontaktní osoba pro bezpečnost na straně Dodavatele nejpozději do 30 dnů od účinnosti této Přílohy potvrdila písemně Objednateli, že všechny osoby podílející se na poskytování plnění dle Dohody za stranu Dodavatele a/nebo jeho poddodavatelé byli prokazatelně seznámeni s těmito Bezpečnostními požadavky.



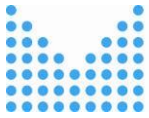
4. Dodržovat příslušná ustanovení bezpečnostních politik, metodik a postupů předaných Dodavatelí Objednatelem, k jejichž dodržování se Dodavatel zavázal, pokud byl Dodavatel s takovými dokumenty nebo jejich částmi seznámen, a to bez ohledu na způsob, jakým byl s takovou dokumentací Objednatele seznámen (např. školením, protokolárním předáním příslušné dokumentace dodavatelí, elektronickým předáním prostřednictvím e-mailu či datovou schránkou, zřízením přístupu Dodavatelí na sdílené úložiště aj.).
5. Rozvíjet bezpečnostní povědomí svých zaměstnanců a příp. dalších osob, které se podílejí na plnění dle Dohody a průběžně je seznamovat s prováděnými nebo plánovanými změnami. Zaměstnanci a další osoby na straně Dodavatele podílející se na plnění dle Dohody musí být prokazatelně seznámeni s platnými předpisy a bezpečnostními požadavky Objednatele, a to ještě před zahájením jakékoli činnosti ze strany těchto osob pro Objednatele v souvislosti s plněním dle Dohody.
6. Zaznamenávat a na vyžádání Objednateli poskytnout veškeré podstatné okolnosti související s poskytovaným předmětem plnění dle Dohody (technické záznamy, organizační záznamy o školení, pověření apod.).
7. Přidělovat svým jednotlivým pracovníkům oprávnění k výkonu činností a přísně při tom dodržovat bezpečnostní zásadu tzv. „potřeba vědět“ (need-to-know principle), tedy zejména dbát o to, aby byla minimalizována rizika nežádoucího přístupu k aktivům Objednatele.
8. Zajistit dostatečnou míru zastupitelnosti pro technické aspekty řešení (zajištění kontinuity dodávky, zastupitelnost pracovníků, zejména Kontaktní osoba pro bezpečnost na straně Dodavatele).

2.3. Oprávnění užívat data

1. Dodavatel je při poskytování plnění pro Objednatele oprávněn nakládat s daty předanými Dodavatelí Objednatelem výhradně za účelem plnění předmětu Dohody, avšak vždy pouze v rozsahu nezbytném ke splnění předmětu Dohody resp. Prováděcí smlouvy.
2. Dodavatel se při poskytování plnění pro Objednatele zavazuje nakládat s daty pouze v souladu s Dohodou, Prováděcí smlouvou a příslušnými právními předpisy, zejména ZKB, VKB a dalšími souvisejícími právními předpisy.

2.4. Kontrola souladu s požadavky bezpečnosti

1. Dodavatel je srozuměn s prováděním hodnocení rizik, kontrolou a auditem zavedených bezpečnostních opatření ze strany Objednatele v souvislosti s poskytovanou službou Dodavatelem.
2. Hodnocení, kontrola a audit probíhají v intervalech stanovených Objednatelem nebo v případě vzniku kybernetického bezpečnostního incidentu v rámci poskytované služby nebo v případě, že se vznik bezpečnostního incidentu jeví jako pravděpodobný. Kontrola nebo audit mohou být provedeny v prostorách Dodavatele nebo jeho poddodavatele a Dodavatel má povinnost tyto kontroly a audity Objednateli či Objednatelem pověřené osobě umožnit či možnost jejich provedení v prostorách poddodavatele zajistit, přispět k nim a poskytnout Objednateli či Objednatelem pověřené osobě k jejich provedení maximální možnou součinnost, kterou lze po Dodavatelí rozumně požadovat. Počet a frekvence kontrol ani auditů nejsou nijak omezeny s tím, že náklady Dodavatele



s poskytnutím součinnosti při kontrole hradí Objednatel, a to dle MD sazby a počtu skutečně vykázaných MD dle aktuální ceny MD, která je uvedena v Dohodě.

3. Dodavatel je povinen po zavedení opatření provést také vlastní hodnocení rizik a kontrolu zavedených bezpečnostních opatření. Tato kontrola probíhá v intervalech stanovených v rámci systému řízení Dodavatele, na žádost Objednatele nebo v případě vzniku kybernetického bezpečnostního incidentu v rámci poskytované služby nebo v případě, že se vznik bezpečnostního incidentu jeví jako pravděpodobný. O výsledku kontroly vyžádané Objednatelem podá Dodavatel Objednateli bez zbytečného odkladu písemnou kontrolní zprávu s tím, že náklady Dodavatele spojené se zavedením opatření hradí Objednatel, a to dle MD sazby a počtu skutečně vykázaných MD dle aktuální ceny MD, která je uvedena v Dohodě.

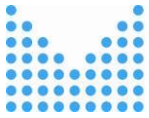
2.5. Řetězení a řízení dodavatelů

Dodavatel se při poskytování plnění pro Objednatele zavazuje plnit následující povinnosti:

1. Dodavatel nezapojí do poskytování plnění dle Dohody žádného dalšího poddodavatele bez předchozího konkrétního písemného povolení Objednatele;
2. Dodavatel se zavazuje, že se bude řídit požadavky Objednatele na řízení bezpečnosti informací a poskytne Objednateli veškerou nezbytnou součinnost v otázkách řízení bezpečnosti informací a pokud využívá při poskytování plnění poddodavatele, zajistí, že bude Objednateli poskytnuta veškerá nezbytná součinnost v otázkách řízení bezpečnosti informací také od těchto poddodavatelů.
3. Dodavatel je povinen předat Objednateli kontaktní údaje všech osob dodávajících systémovou a technickou podporu pro řešení.
4. Pokud Dodavatel využívá při poskytování plnění poddodavatele, zavazuje se, že budou dodržovat bezpečnostní požadavky vč. požadavků na ochranu osobních údajů vyplývající z této Přílohy, Dohody nebo Prováděcí smlouvy. Dodavatel se zavazuje bezodkladně doložit Objednateli na základě jeho výzvy smluvní dokumenty se svými poddodavateli, ze kterých bude vyplývat závazek poddodavatele poskytovat plnění v souladu s bezpečnostními požadavky vyplývajícími z této Přílohy, Dohody nebo Prováděcí smlouvy.
5. Dodavatel odpovídá za to, že jeho poddodavatelé nebudou jednat v rozporu s bezpečnostními požadavky vyplývajícími z této Přílohy; v případě, že dojde k nedodržení těchto požadavků ze strany poddodavatele Dodavatele, považuje se každé takové nedodržení požadavků za porušení povinnosti Dodavatele dle Dohody.

2.6. Povinnosti v řízení změn dle ZKB a VKB

1. Dodavatel se zavazuje v rozsahu předmětu plnění aktivně podílet na splnění povinností v oblasti řízení změn dle ZKB a VKB, zejména při analýze souvisejících rizik, přijímání opatření za účelem snížení všech nepříznivých dopadů spojených se změnami, aktualizací bezpečnostní dokumentace, souvisejícím testováním a zajištění možnosti návratu do původního stavu.
2. Dodavatel se minimálně zavazuje v rozsahu předmětu plnění na své straně přiměřeně reagovat na změny a upravit na své straně technická a organizační opatření tak, aby odpovídala novému stavu po provedení změny. Náklady Dodavatele se zavedením technických a organizačních opatření hradí Objednatel tím, že rozsah těchto změn a jejich



cena bude vždy předem stanovena Dodavatelem v samostatné nabídce a potvrzena Objednatelem v navazující objednávce.

3. Dodavatel se zavazuje aktivně spolupracovat při testování významné změny.

2.7. Zvládání bezpečnostních událostí a incidentů

Dodavatel se při poskytování plnění pro Objednatele zavazuje, že:

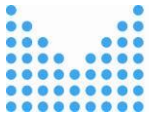
1. Stanoví činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládnutí bezpečnostních událostí a incidentů, bude postupovat podle správcem stanovených a popsáných pravidel, a bude hlásit všechny bezpečnostní události a incidenty neprodleně po jejich detekci Objednateli prostřednictvím ohlašovacích kanálů Objednatele, v případech, kdy situace nestrpí odklad telefonicky. Dále se zavazuje vyhodnotit informace o bezpečnostních událostech a incidentech a o těchto informacích, vzniklých bezpečnostních incidentech, vč. krátkodobých a dlouhodobých nápravných opatřeních nad všemi částmi řešení, které jsou ve správě Dodavatele, a rizicích souvisejících s ohrožením kontinuity činností vést záznamy a tyto uchovat pro jejich budoucí použití s ohledem na požadavky Objednatele a legislativy ČR. Nastavená pravidla a postupy podléhají schválení Objednatelem.
2. Bude respektovat nastavená pravidla pro zvládnutí bezpečnostních incidentů včetně požadavku na legalitu zajištění stop, tj. jejich původ a oprávněnost jejich získání musí být v souladu s platnými zákony a standardy tak, aby bylo možné jejich následné využití v rámci forenzní analýzy a eventuální použití jako důkazní materiál.
3. Provede analýzu příčin bezpečnostního incidentu a navrhne opatření s cílem zamezit jeho opakování.

2.8. Informační povinnost a povinnosti při výměně informací

1. Dodavatel se během poskytování plnění zavazuje Objednatele informovat o:
 - a) Způsobu řízení rizika bez zbytečného odkladu také o změnách ve způsobu řízení rizik.
 - b) Významné změně ovládnutí Dodavatele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných Dodavatelem k plnění na základě smluvního vztahu s Objednatelem.
2. Dodavatel se během poskytování plnění pro Objednatele zavazuje dostatečně zabezpečit veškerý přenos dat a informací z pohledu bezpečnostních požadavků na jejich důvěrnost a integritu před hrozbami v kybernetické bezpečnosti v souladu s ZKB a VKB, nebo pokud nebude dohodnuto jinak.

2.9. Bezpečnost lidských zdrojů

1. Dodavatel připraví za součinnosti Objednatele poučení pro seznámení všech stran podílejících se na poskytování předmětu plnění s pravidly, která musí být v průběhu dodávky dodržována. Dodavatel zajistí jejich dodržování nasazením kontrolních a vynucovacích mechanismů. Rozsah poučení podléhá schválení Objednatele.



2.10. Fyzická ochrana a bezpečnost prostředí

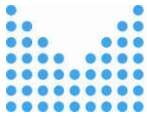
1. Dodavatel se zavazuje dodržovat provozní řády budov (režimová opatření) a využívaných prostor, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny komponenty technologických a komunikačních systémů, anebo datové nosiče (dále také jen „Pracoviště“).
2. Dodavatel se zavazuje, že na Pracovišti neponechá volně dostupná instalační, záložní nebo archivní média ani dokumentaci k předmětu plnění dle Dohody.

2.11. Požadavky na Řízení přístupu

1. Dodavatel bere na vědomí, že přístup k datům, informacím či zařízením souvisejícím s předmětem plnění dle Dohody je možné povolit pouze konkrétním fyzickým osobám / zaměstnancům Dodavatele / poddodavatele Dodavatele, a to na základě požadavku Dodavatele na přístup.
2. Dodavatel bere na vědomí, že přidělení oprávnění zaměstnanci Dodavatele musí být řízeno zásadou tzv. „potřeba vědět“ (need-to-know principle).
3. Dodavatel se zavazuje, že udělený přístup nesmí být sdílen více zaměstnanci Dodavatele nebo poddodavatele Dodavatele.
4. Dodavatel se zavazuje, že nebude instalovat a používat žádné nástroje, které nebyly předem písemně odsouhlaseny Objednatelem.
5. Dodavatel se zavazuje, že nebude vyvíjet, kompilovat a šířit v jakékoliv části technologického nebo komunikačního systému programový kód, který má za cíl nelegální ovládnutí, narušení, nebo diskreditaci technologického nebo komunikačního systému nebo nelegální získání dat a informací. Dodavatel bere na vědomí, že přístup do interní sítě Objednatele a/nebo k technologickým a komunikačním systémům Objednatele bude realizován výhradně způsobem schváleným Objednatelem.
6. Dodavatel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli, a které přistupují do interní sítě a/nebo technologického nebo komunikačního systému, chránili autentizační prostředky a údaje k systémům Objednatele. Dodavatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako bezpečnostní incident ve smyslu příslušné řídicí dokumentace a mohou být uplatněny příslušné postupy zvládnutí bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům fyzických osob externího subjektu platí pro Dodavatele, pokud byl s takovou řídicí dokumentací Objednatele seznámen).
7. Dodavatel bere na vědomí, že postup zvládnutí bezpečnostního incidentu či skutečnosti vzniklé v důsledku porušení Bezpečnostních požadavků nebudou posuzovány jako okolnost vylučující odpovědnost Dodavatele za prodlení s řádným a včasným plněním předmětu Dohody, resp. Prováděcí smlouvy a nebudou důvodem k jakékoli náhradě případné újmy Dodavateli či jiné osobě ze strany Dodavatele. Ostatní ustanovení ohledně odpovědnosti Dodavatele za prodlení obsažená v Dohodě nejsou tímto ustanovením dotčena.

2.12. Monitorování činností

1. Dodavatel bere na vědomí, že veškerá aktivita Dodavatele a jeho plnění realizované v rámci plnění předmětu Dohody nebo s ním úzce související budou Objednatelem



průběžně a pravidelně monitorovány a vyhodnocovány s ohledem na obsah Dohody, resp. Prováděcí smlouvy a interních dokumentů Objednatele.

2.13. Předání a převzetí plnění

1. Dodavatel se zavazuje dodržovat Bezpečnostní požadavky i při předání a převzetí plnění dle Dohody, resp. Prováděcí smlouvy.
2. Objednatel je oprávněn z důvodu nedodržení Bezpečnostních požadavků včetně požadavku na předání Bezpečnostní dokumentace odmítnout převzetí (části) plnění dle Dohody, resp. Prováděcí smlouvy.

2.14. Likvidace dat

Dodavatel se zavazuje plnit požadavky Objednatele v oblasti likvidace dat (ať už dat na papírových médiích, dat zpracovávaných elektronicky nebo prostřednictvím jakýchkoli dalších nosičů dat) dle přílohy č. 4 VKB.

2.15. Sankce

Sankce za porušení povinností plynoucích z bezpečnostních opatření a ZKB a VKB jsou uvedeny v Dohodě.